RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: SBV-M01

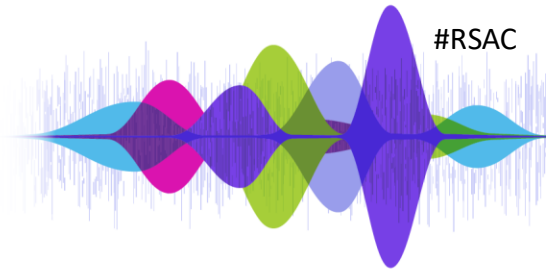
RSAC PicoCTF: Driving Year-Round Community Engagement

David Brumley

CEO and Professor
Mayhem Security and Carnegie Mellon University
https://www.linkedin.com/in/thedavidbrumley/

John Hammond

Principle Security Researcher
Huntress, Inc.
https://www.linkedin.com/in/johnhammond010/



Disclaimer

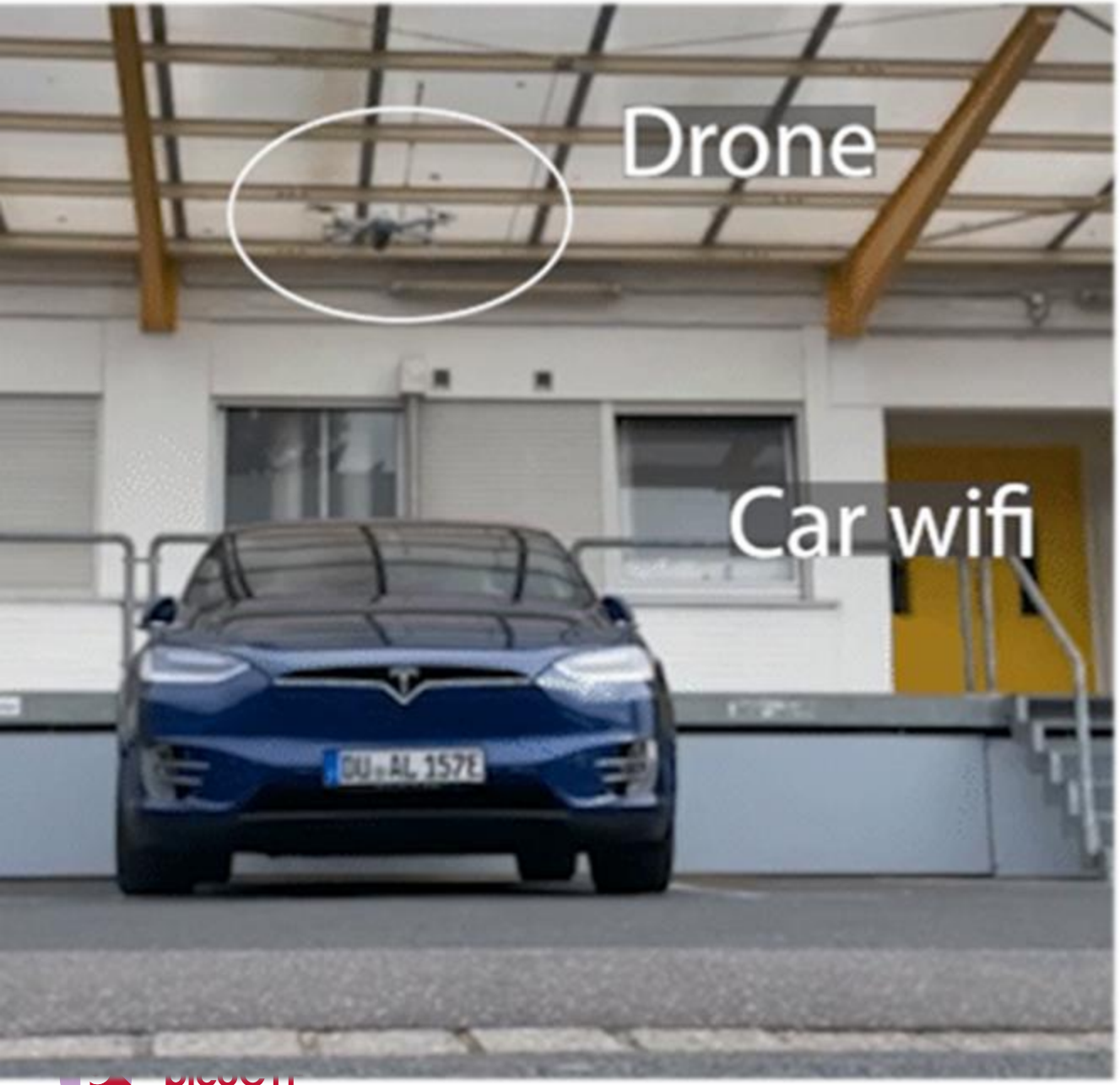
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

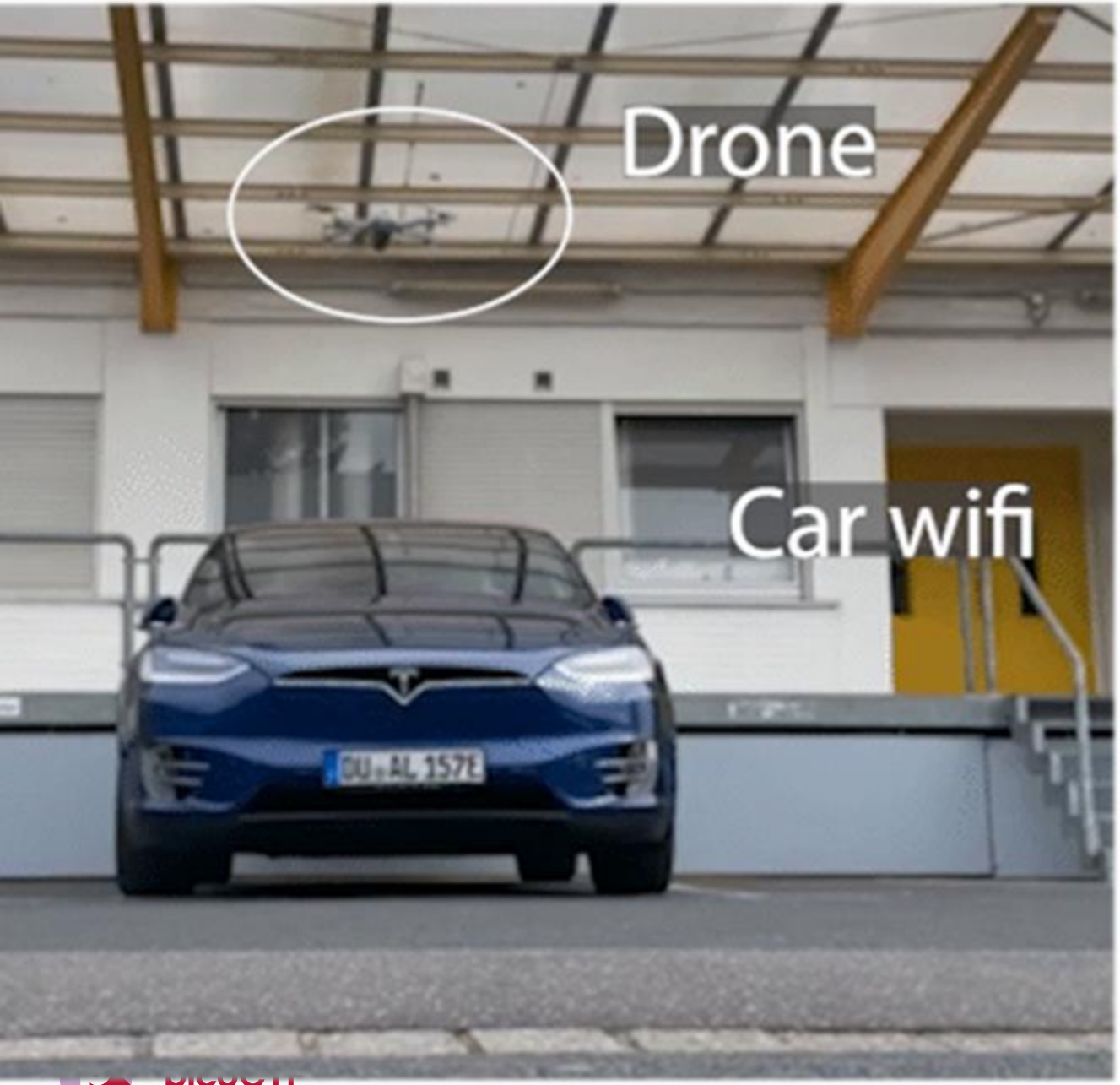
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Geohotz
Comma.ai

How do people become **ELITE HACKERS?**

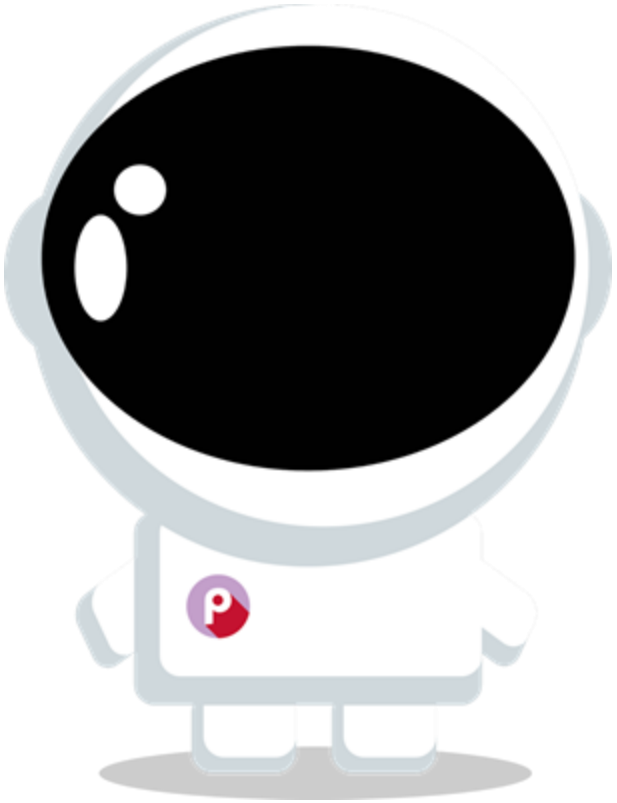


HOW **DID THEY** DO THAT?

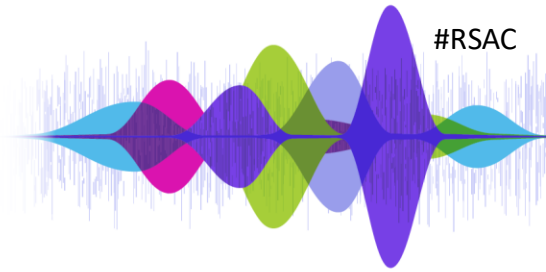


HOW
CAN I
DO THAT?

Romantic but
not real



Self Learning with Capture The Flag



01: CTF IS DELIBERATE PRACTICE

20% complete

Excellence demands effort and planned, deliberate practice of increasing intensity

K. Anders Ericsson

PERFORMANCE SCIENCE

Specific Skill

Specific Goal

Immediate Feedback

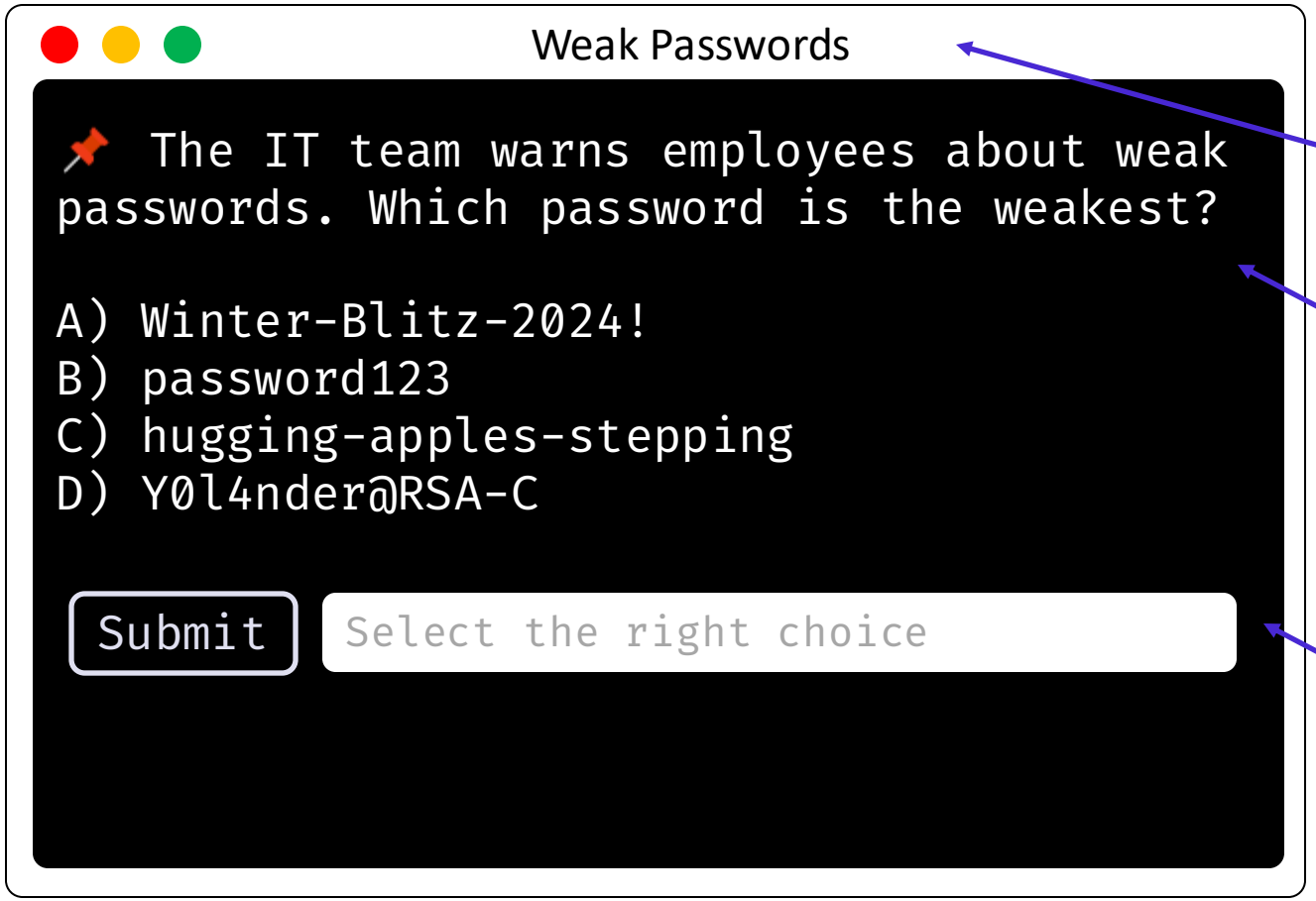
Repetition

Increasing Difficulty

RSAC PicoCTF

https://rsac.picoctf.org

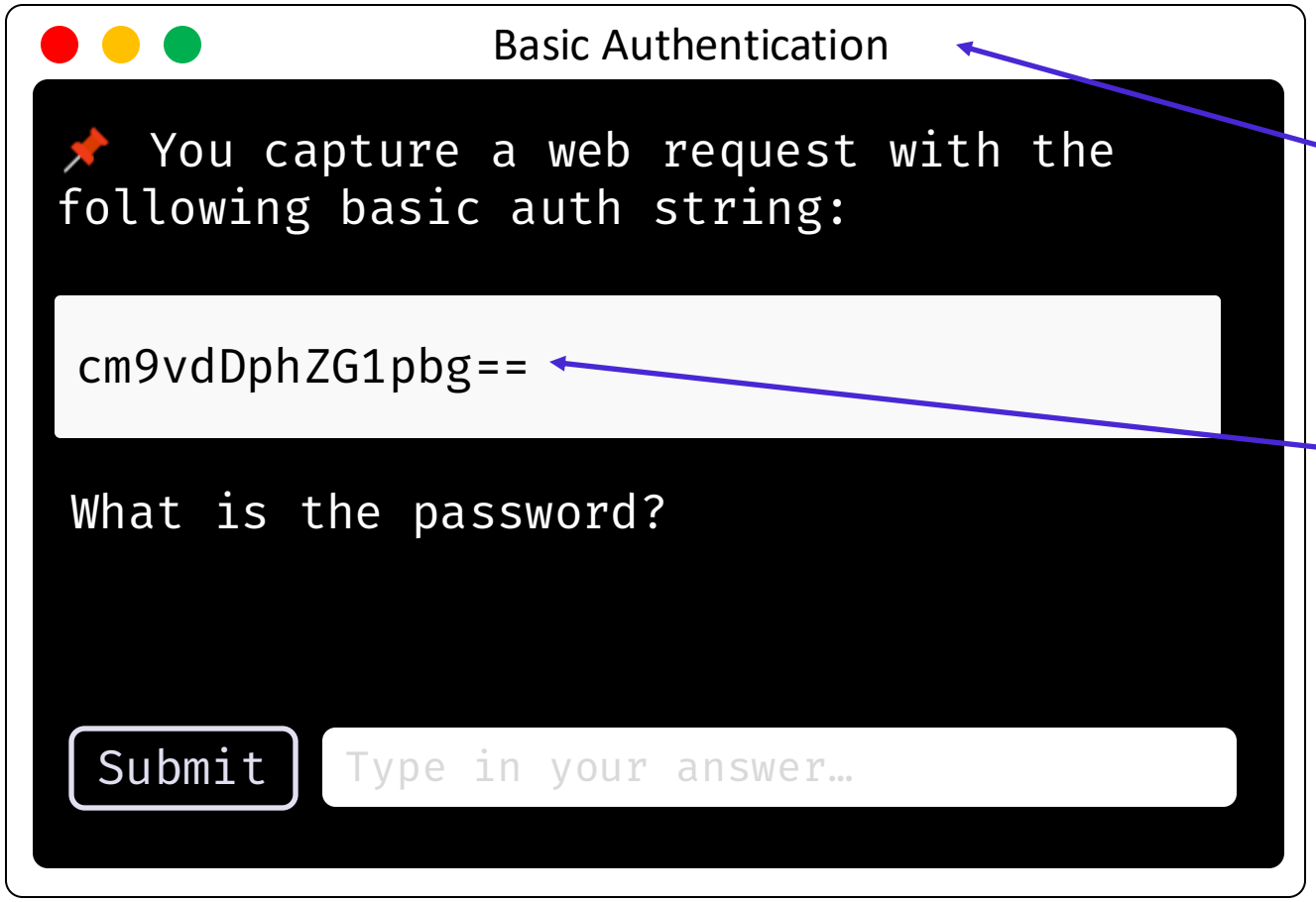
Hack, Play, and Level Up with RSAC PicoCTF



Specific skill

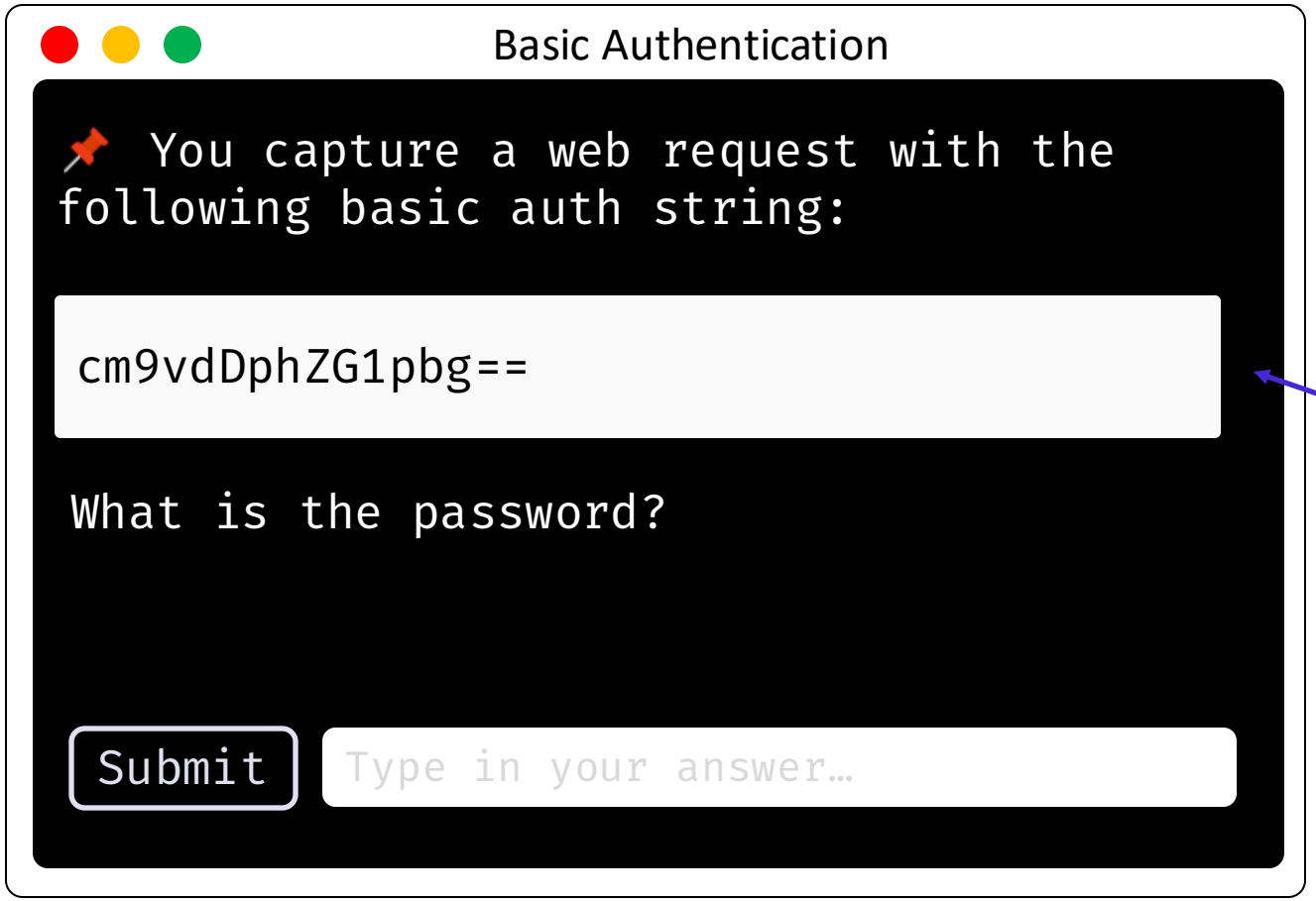
Specific goal

Feedback


Basic Authentication
📌 You capture a web request with the following basic auth string:
cm9vdDphZG1pbg==
What is the password?
Submit
Type in your answer…

Building on skills

What the heck is that?


Basic Authentication
📌 You capture a web request with the following basic auth string:
cm9vdDphZG1pbg==
What is the password?
Submit
Type in your answer…

💪🧠🔨New skill:
Recognize base64

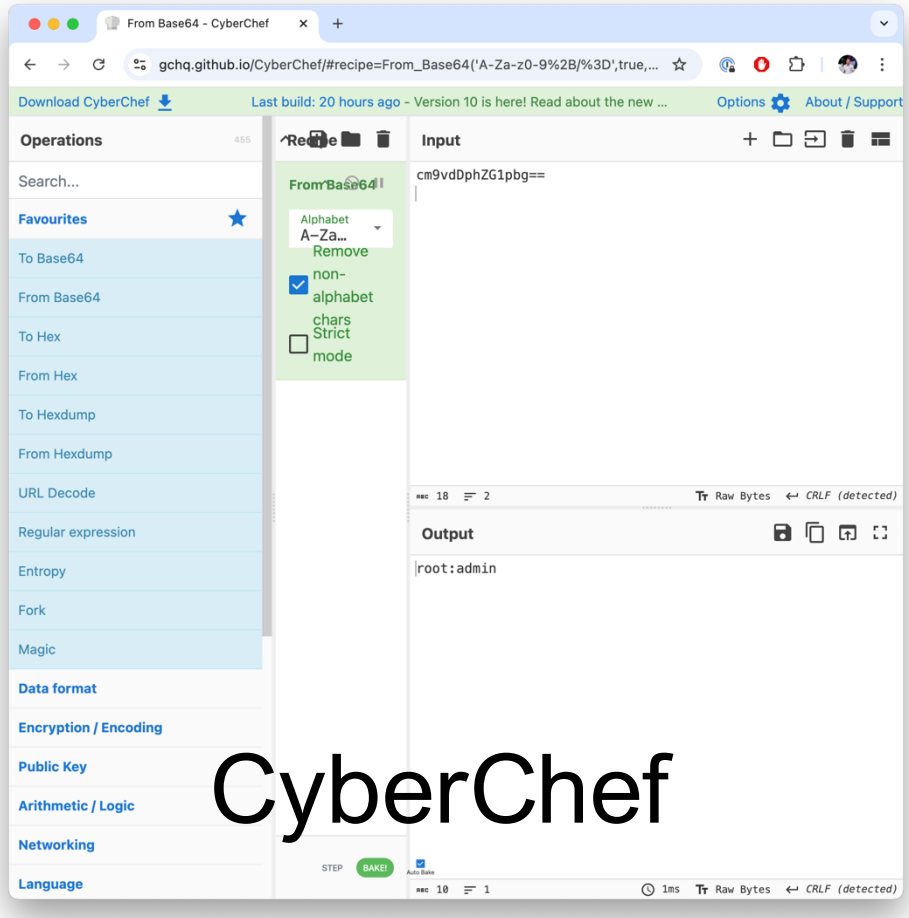
Basic Authentication

📌 You capture a web request with the following basic auth string:

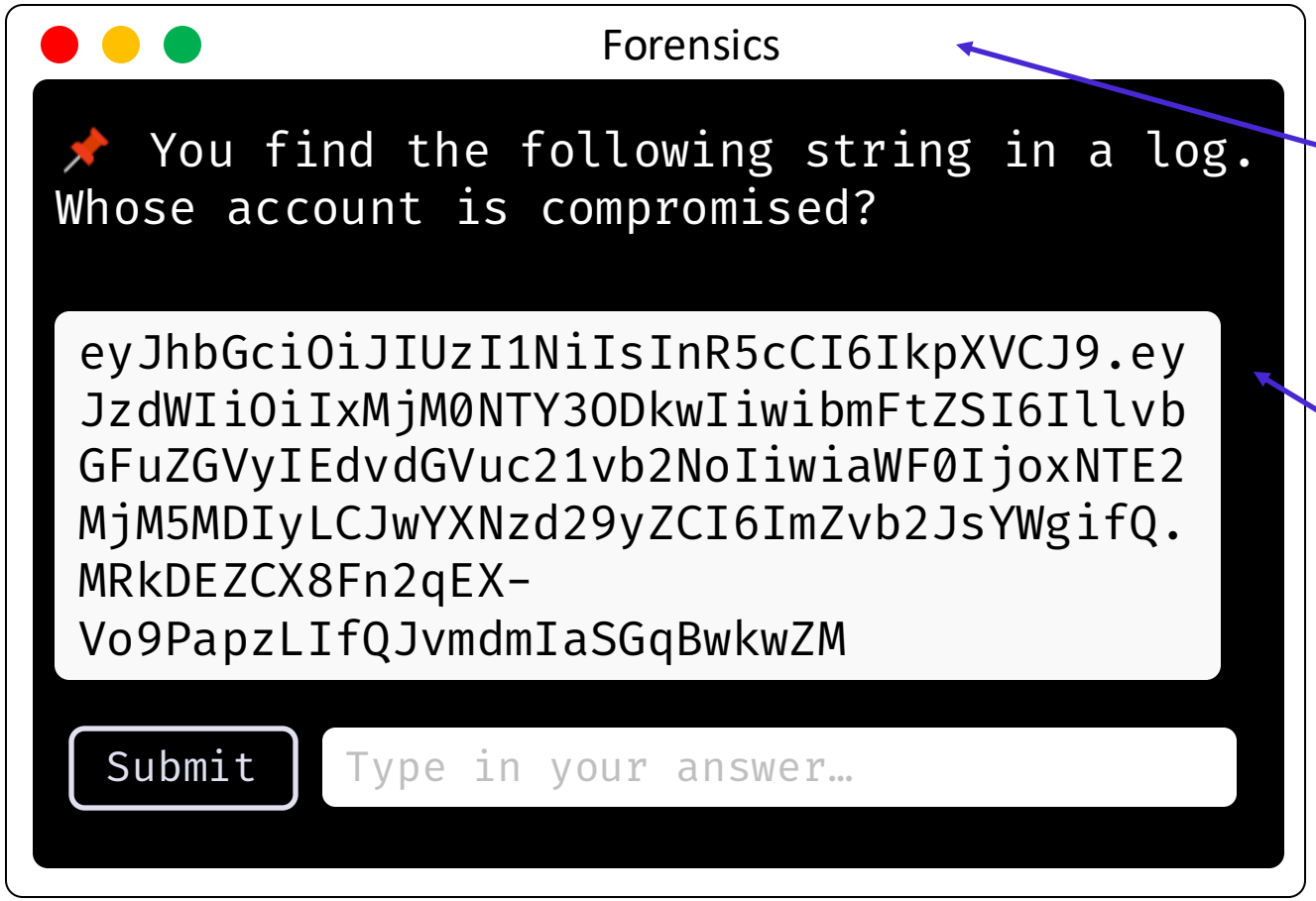
```
cm9vdDphZG1pbg==
```

What is the password?

Submit `root:admin`



CyberChef


Forensics
📌 You find the following string in a log. Whose account is compromised?
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IllvbGFuZGVyIEdvdGVuc21vb2NoIiwiaWF0IjoxNTE2MjM5MDIyLCJwYXNzd29yZCI6ImZvb2JsYWgifQ.MRkDEZCX8Fn2qEX-Vo9PapzLIfQJvmdmIaSGqBwkwZM
Submit
Type in your answer…

more building..

💪🧠🔨 New skill: Recognize JWT
(three base64 encoded strings with “.” separating)

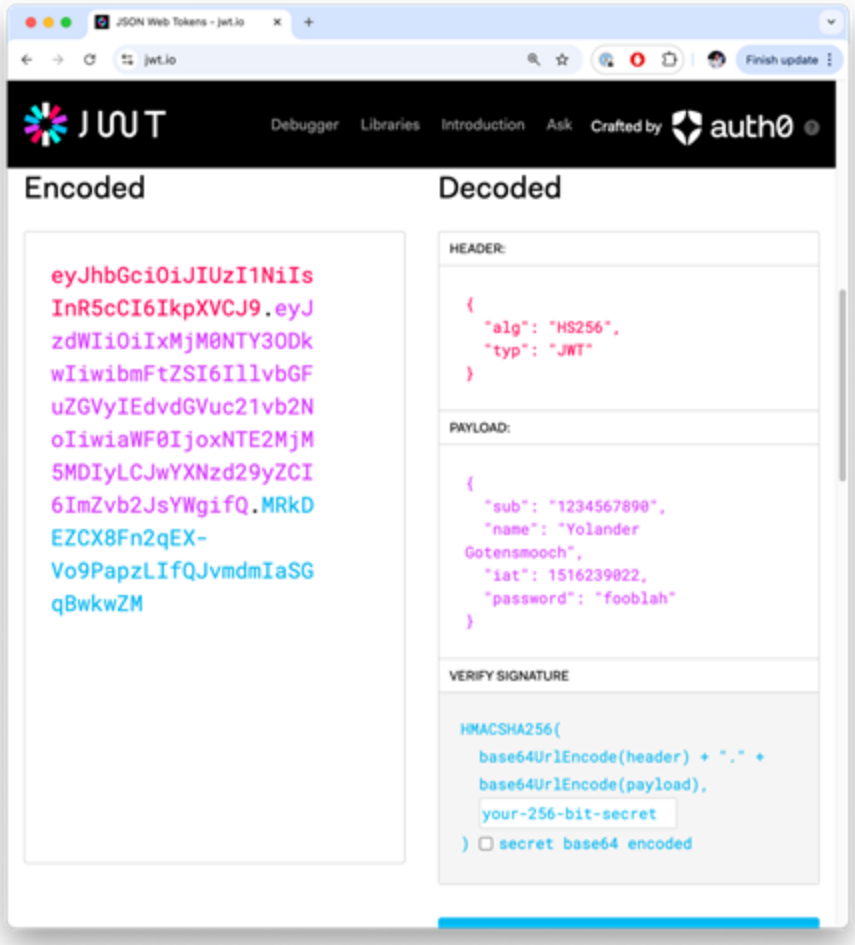
Forensics

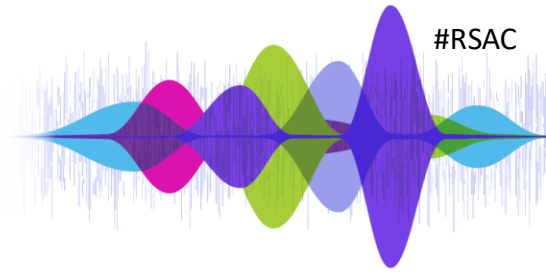
📌 You find the following string in a log. Whose account is compromised?

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IllvbGFuZGVyIEdvdGVuc21vb2NoIiwiaWF0IjoxNTE2MjM5MDIyLCJwYXNzd29yZCI6ImZvb2JsYWgifQ.MRkDEZCX8Fn2qEX-Vo9PapzLIfQJvmdmIaSGqBwkwZM
```

Submit

Yolander Gotensmooch





Incremental Mastery

1. Basic password security
2. Recognize password encoding
3. Apply to insecure JWT

Build your toolbox

Tech	Example	Tool
Base64	cm9vdDphZG1pbg==	Cyberchef
JWT	Three base64 with “.”	JWT.io
Hex	72 6f 6f 74 3a 61 64 …	Cyberchef/ python

Effective

Classroom

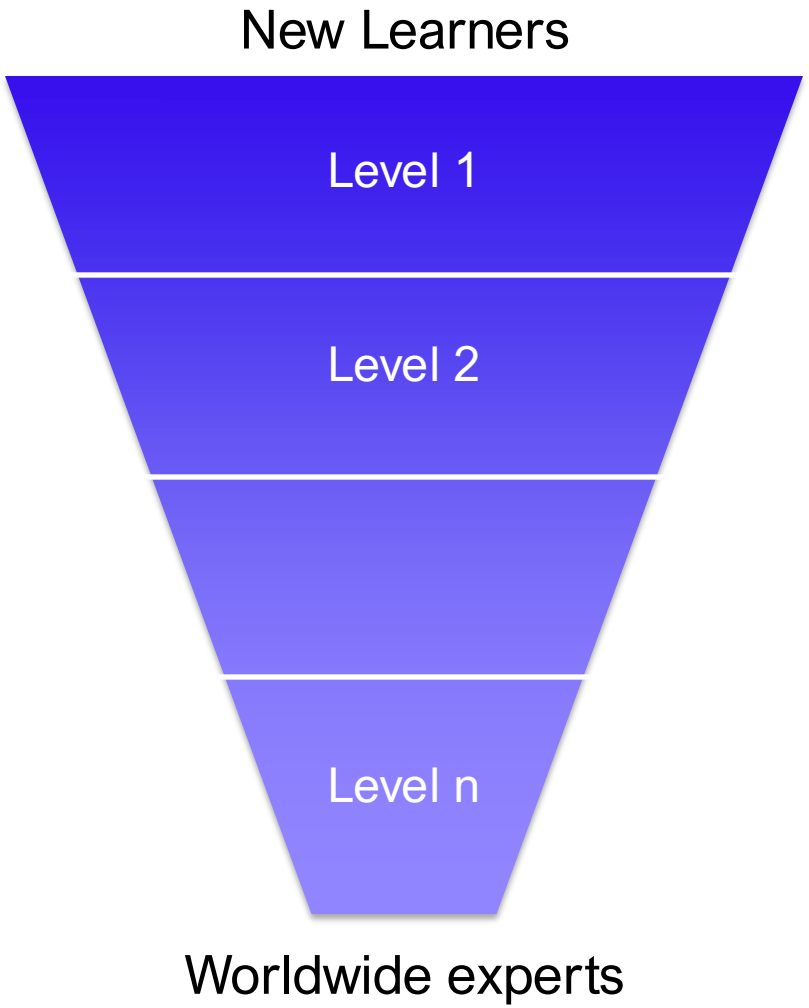
CTFs

Fun

Textbooks

Founders, Executives, Leaders, Hackers

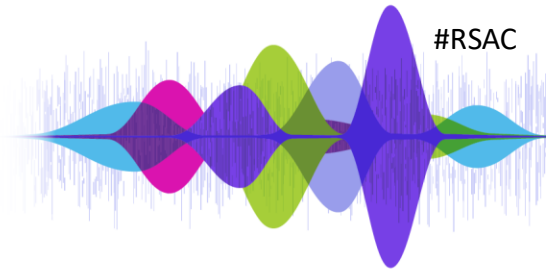
Geohotz	Hudson	Erye	x1on	Fluorescence
Founder Comma.ai	Amazon CISO	Google Threat Intel	$1m+ bounty	$1m+ bounty



PicoCTF.org

CMU's approach to building cybersecurity talent for the last decade.

DEFCON32.CTF
Maple Mallard
August 8-11, 2024
Vegas, Nevada, USA



02: CTF TO CVE

John Hammond

50% complete

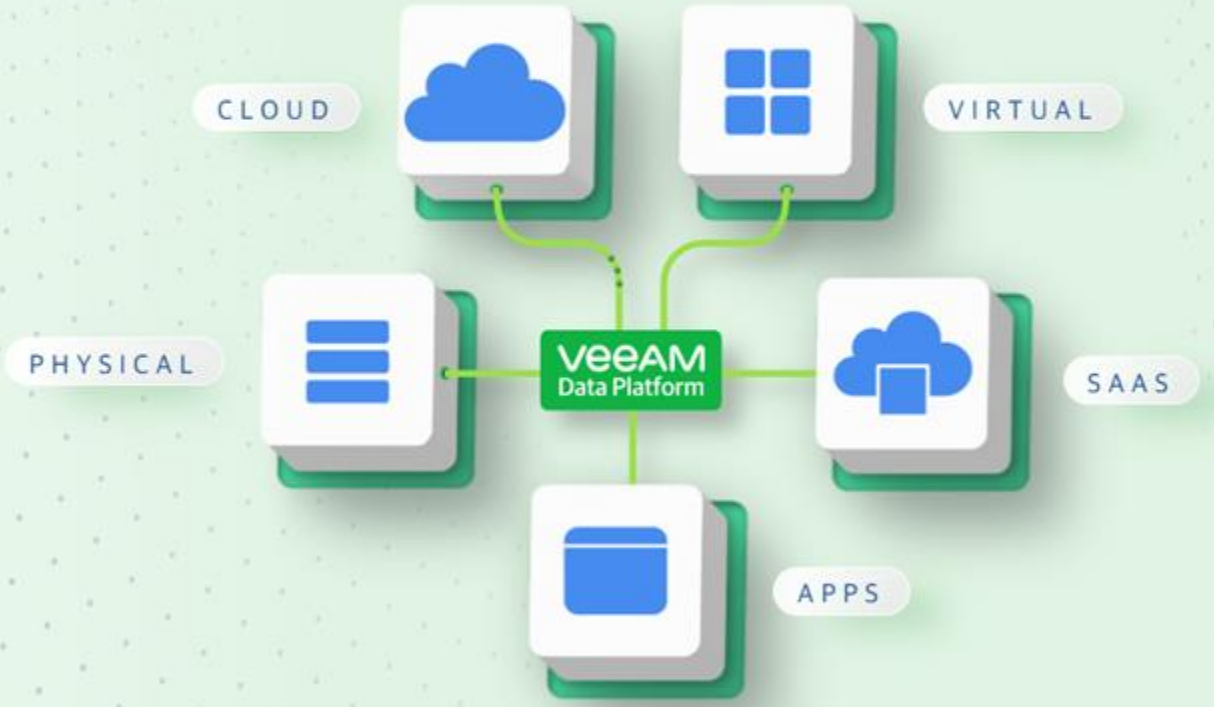
CYBERSTAKES
John 'da ROPper

We Keep Your Business Running

#1 Modern Data Protection

Providing data resiliency through secure backup and fast, reliable recovery solutions for your hybrid cloud.

LEARN MORE



https://www.veeam.com/

https://www.veeam.com/kb4424

CVE-2023-27532

KB ID: 4424

Product: Veeam Backup & Replication
Veeam Backup & Replication *Community Edition*

Published: 2023-03-07

Last Modified: 2023-03-10

https://www.veeam.com/kb4424

Challenge

Vulnerability CVE-2023-27532 in a Veeam Backup & Replication component allows an unauthenticated user operating within the backup infrastructure network perimeter to obtain encrypted credentials stored in the configuration database. This may lead to an attacker gaining access to the backup infrastructure hosts.

Severity: High

CVSS v3 score: 7.5

https://www.veeam.com/kb4424

Challenge

Vulnerability CVE-2023-27532 in a Veeam Backup & Replication component allows an unauthenticated user operating within the backup infrastructure network perimeter to obtain encrypted credentials stored in the configuration database. This may lead to an attacker gaining access to the backup infrastructure hosts.

Severity: High

CVSS v3 score: 7.5

Cause

The vulnerable process, Veeam.Backup.Service.exe (TCP 9401 by default), allows an unauthenticated user to request encrypted credentials.

Cause

The vulnerable process, Veeam.Backup.Service.exe (TCP 9401 by default), allows an unauthenticated user to request encrypted credentials.

CVE-2023-27532

KB ID: 4424

Product: Veeam Backup & Replication
Veeam Backup & Replication *Community Edition*

Published: 2023-03-07

Last Modified: 2023-03-10

Get weekly article updates

Enter email

SUBSCRIBE

By subscribing, you are agreeing to have your personal information managed in accordance with the terms of Veeam's Privacy Notice.

Challenge

Vulnerability CVE-2023-27532 in a Veeam Backup & Replication component allows an unauthenticated user operating within the backup infrastructure network perimeter to obtain encrypted credentials stored in the configuration database. This may lead to an attacker gaining access to the backup infrastructure hosts.

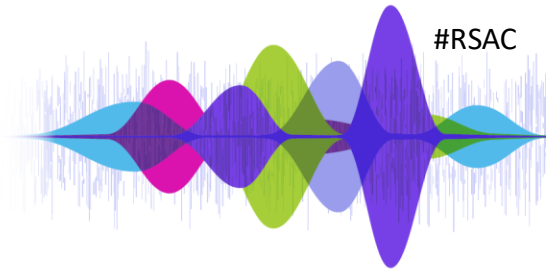
Severity: High
CVSS v3 score: 7.5

Solution

This vulnerability is resolved in the following Veeam Backup & Replication build numbers:

- 12 (*build 12.0.0.1420* ***P20230223***)
- 11a (*build 11.0.1.1261* ***P20230227***)

encrypted credentials.



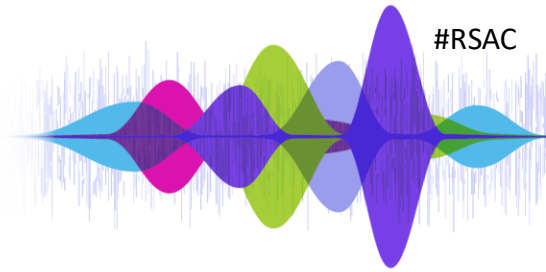
03: HOW TO START

90% complete

April 28 – May 1 Contest

1. Enroll with OneRSAC account
2. RSAC App Community
3. RSAC recognition for winners

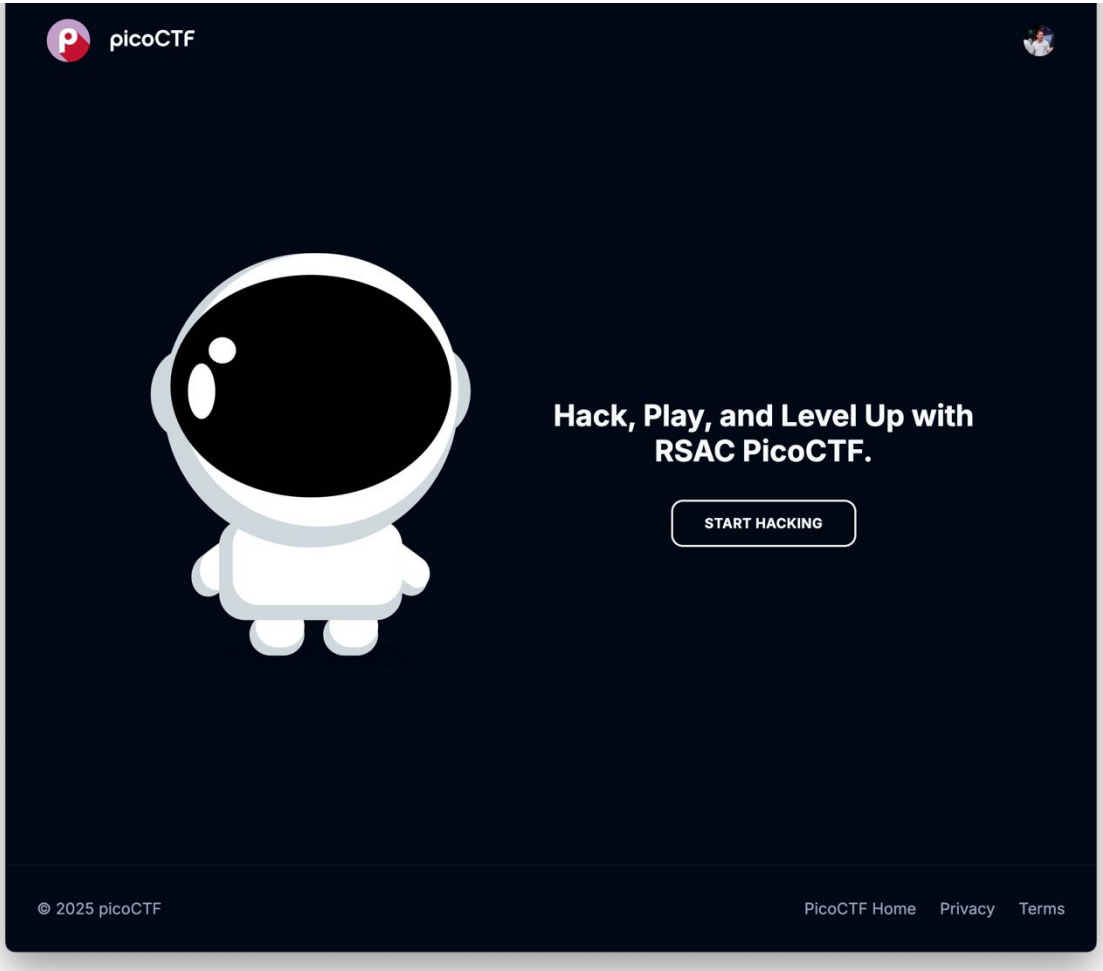
📅 **Persistent year-round access after contest**



06 STARTING NOW

99% complete

Apply Slide

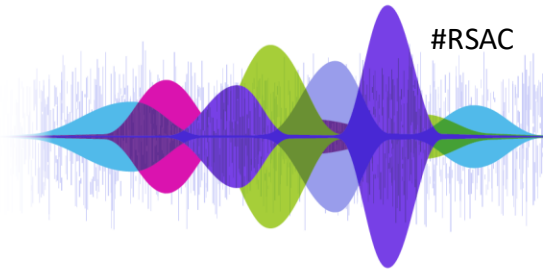


- Go to https://rsac.picoctf.org
- Log in with your OneRSAC
- Hack, Play, and Level Up

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You



“Apply” Slide

- Bullet point here (see slides 7 – 10 for instructions)
- Bullet point here
- Bullet point here

After a major cancer surgery, I realized more than ever the importance of paying it forward.

Education. Community. Opportunity.

RSAC PicoCTF

https://rsac.picoctf.org

Hack, Play, and Level Up with RSAC PicoCTF